

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA

**IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
INSTAGRAM ACCOUNTS YFG.HUNCHO  
AND HUNCHO2LITT THAT ARE STORED  
AT PREMISES CONTROLLED BY META  
PLATFORMS, INC.**

Case No. 24-26-N

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Joseph Simmons, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Instagram account that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. ("Meta"), a social media services company headquartered at 1601 Willow Road, Menlo Park, CA. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the account. The information to be disclosed by Meta and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I have been a Special Agent with the FBI since 2018. My duties as an FBI Special Agent include investigating violations of federal law to include investigations related to public corruption, financial crimes, narcotics trafficking, bank robberies, and gang activity, among others. I have also received training on obtaining and reviewing electronic records, including social media data and telephonic communications.

3. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained

from various law enforcement personnel and witnesses. I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary for the limited purpose of establishing probable cause to conduct a search of and for the items described in Attachments A and B for evidence, contraband, and/or instrumentalities of the criminal conduct described herein. Additionally, unless otherwise indicated, wherever in this Affidavit I assert that an individual made a statement, that statement is described in substance herein and is not intended to be a verbatim recitation of such statement. Furthermore, unless otherwise indicated, all statements contained in this Affidavit are summaries in substance and in part. The following is true to the best of my knowledge and belief.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C § 922 and 924: Shipping, Transporting, Receiving, or Possessing Firearms or Ammunition, 18 U.S.C § 924(c)(1): Use of a firearm in furtherance of a drug trafficking, 21 U.S.C. § 841(a)(1): Manufacturing, Distributing, Dispensing or Possessing With Intent to Manufacture, Distribute or Dispense Controlled Substances, and 21 U.S.C. § 846: Conspiracy to Commit a Title 21 Offense have been committed, are being committed, AND/OR will be committed by HUNTER LEE POWELL or unknown suspects associated with the information to be searched. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

#### **JURISDICTION**

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

#### **FACTS ESTABLISHING PROBABLE CAUSE**

6. The FBI and other federal, state, and local agencies have been investigating the recent acquisition, possession, and use of Machinegun Conversion Devices in the Mobile area. Based on my training and experience, I know that 18 U.S.C. § 922(o) makes it a federal crime for “any person to transfer or possess a machinegun.” 26 U.S.C. 5845(b) of the National Firearms Act defines as

machinegun as “any weapon which shoots, is designed to shoot, or can be readily restored to shoot, automatically more than one shot, without manual reloading, by a single function of the trigger. The term shall also include the frame or receiver of any such weapon, any part designed and intended solely and exclusively, or combination of parts designed and intended, for use in converting a weapon into a machinegun, and any combination of parts from which a machinegun can be assembled if such parts are in the possession or under the control of a person.” Under this definition, a Glock “switch” is a part which converts a semi-automatic pistol into a fully-automatic firearm, and is thus a machinegun as defined by federal law.

7. In early 2024, CHS-1 notified law enforcement that an individual utilizing the Instagram account **Huncho2litt** was acquiring Glock switches through the black market and re-selling them to individuals in the Mobile area. CHS-1 obtained a photo publicly posted to the **Huncho2litt** Instagram page which CHS-1 then provided to law enforcement, as shown below:



8. As shown above, an individual is shown with several firearms at his feet and significant amounts of cash spread out in front of his face and arrayed on the floor. Additionally, there are four plastic bags located by the individual's feet that appear to contain a green substance consistent with marijuana and two bottles of an unknown substance. In my training and experience, the depiction of cash, apparent marijuana, and bottles of an unknown substance is indicative of narcotics distribution.

9. CHS-1 sent a second photo and identified the individual in the photo as being the same individual who controls the Instagram account **Huncho2litt**, as shown below:



10. The photo depicts a masked individual holding what appears to be a Glock pistol with a “switch” affixed to the rear of the slide. A second pistol is visible tucked under the individual's arm.

11. Also in early 2024, CHS-2 similarly identified the individual utilizing the Instagram accounts **Huncho2litt**, as an individual who was acquiring and selling Glock “switches.” CHS-2 identified a second Instagram account, **Yfg.Huncho** as being controlled by the same individual. CHS-2

knew that the individual's first name was "Hunter" and that he has a nickname of "Head Huncho." CHS-2 indicated that he/she has known "Hunter" for approximately two years. During this time, CHS-2 has known "Hunter" to sell marijuana and other controlled substance, in addition to Glock switches, which is corroborated by the above photo depicting cash, bags of apparent marijuana, and bottles of an unknown substance posted on the **Huncho2Litt** Instagram account. On one occasion near when they first met, "Hunter" showed CHS-2 a Glock pistol equipped with a "switch." "Hunter" offered to sell the pistol and "switch" to CHS-2, but CHS-2 declined.

12. Both CHS-1 and CHS-2 have known "Hunter" for several years and interacted with him in-person on numerous occasions. Through these in-person interactions, CHS-1 and CHS-2 have confirmed that "Hunter" is the individual controlling the Instagram accounts **Huncho2Litt** and **Yfg.Huncho**.

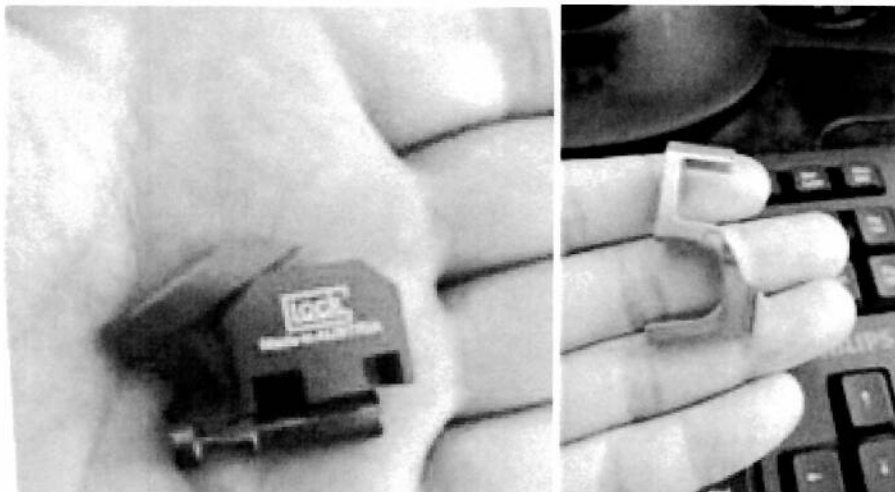
13. Based on the information provided by CHS-1 and CHS-2, law enforcement were able to identify the individual controlling the Instagram accounts as HUNTER LEE POWELL ("POWELL"). Photographs posted on these accounts matched the photographs of the exterior of the residence listed on HUNTER POWELL's Alabama driver's license. Additionally, a review of HUNTER POWELL's Alabama driver's license photo and those from the **Huncho2Litt** and **Yfg.Huncho** Instagram accounts appear to depict the same person.

14. CHS-2 re-established contact with POWELL in early 2024 and communicated with him via Instagram account **Yfg.Huncho**. POWELL indicated that he was willing to sell a Glock "switch" to CHS-2 for between \$150 and \$250. POWELL indicated that he had various types of "switches," including "incognito" switches, such that there are no obvious external changes or attachments on the pistol equipped with an "incognito" switch. Additionally, POWELL indicated that he also had for sale Machinegun Conversion Devices that could be used to convert an AR-style semi-automatic rifle into a fully automatic machinegun.

15. POWELL also sent CHS-2 videos of a white, male individual holding and firing Glock pistols equipped with Glock "switches." Based on the context of these exchanges, I believe those photos



and videos depicts POWELL. Screenshots of photos sent by POWELL via Instagram account **Yfg.Huncho** are shown below:



16. POWELL's acquisition, possession, and apparent willingness to sell Machinegun Conversion Devices area a violation of 18 U.S.C. § 922(o). POWELL's possession of firearms while also allegedly selling marijuana, a federally-controlled substance, violates 18 U.S.C § 924(c)(1): Use of a firearm in furtherance of a drug trafficking, 21 U.S.C. § 841(a)(1): Manufacturing, Distributing, Dispensing or Possessing With Intent to Manufacture, Distribute or Dispense Controlled Substances, and/or 21 U.S.C. § 846 Conspiracy statutes. In my training and experience, individuals involved in narcotics trafficking and the distribution of illegal firearms parts often utilize social media, such as Instagram, to further their crimes. Based on the information provided by CHS-1, CHS-2, and a review of the publicly posted images on the Instagram accounts **Yfg.Huncho** and **Huncho2Litt**, I believe these accounts have been utilized and are being utilized by HUNTER LEE POWELL to further his criminal activities. A review of the data associated with Instagram accounts **Yfg.Huncho** and **Huncho2litt** are likely to provide further evidence of these crimes.

**CONFIDENTIAL HUMAN SOURCES**

17. CHS-1 has been cooperating with the FBI since about 2023. Over the period of the investigation described herein, I have found that CHS-1 has provided reliable and credible information based on independent corroboration by law enforcement in this investigation.

18. CHS-2 has been cooperating with the FBI since about 2023. Over the period of the investigation described herein, I have found that CHS-2 has provided reliable and credible information based on independent corroboration by law enforcement in this investigation.

### **PROVIDER BACKGROUND**

19. Instagram is a service owned by Meta, a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510. Specifically, Instagram is a free-access social networking service, accessible through its website and its mobile application, that allows subscribers to acquire and use Instagram accounts, like the target account(s) listed in Attachment A, through which users can share messages, multimedia, and other information with other Instagram users and the general public.

20. The information in this section is based on information published by Meta on its Instagram website, including, but not limited to, the following webpages: “Data Policy,” <https://help.instagram.com/519522125107875>; “Information for Law Enforcement,” <https://help.instagram.com/494561080557017>; and “Help Center,” <https://help.instagram.com>.

21. Meta collects basic contact and personal identifying information from users during the Instagram registration process. This information, which can later be changed by the user, may include the user’s full name, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, credit card or bank account number, and other personal identifiers. Meta keeps records of changes made to this information.

22. Meta also collects and retains information about how each user accesses and uses Instagram. This includes information about the Internet Protocol (“IP”) addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

23. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same usernames at the same time. Instagram users can create multiple accounts and, if “added” to the primary account, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

24. Instagram users can also connect their Instagram and Facebook accounts to utilize certain cross-platform features, and multiple Instagram accounts can be connected to a single Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can “tweet” an image uploaded to Instagram to a connected Twitter account or post it to a connected Facebook account, or transfer an image from Instagram to a connected image printing service. Meta maintains records of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Meta and third-party websites and mobile apps.

25. Instagram users can “follow” other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also “block” other users from viewing their posts and searching for their account, “mute” users to avoid seeing their posts, and “restrict” users to hide certain activity and prescreen their comments. Instagram also allows users to create a “close friends list” for targeting certain communications and activities to a subset of followers.

26. Users have several ways to search for friends and associates to follow on Instagram, such as by allowing Meta to access the contact lists on their devices to identify which contacts are Instagram users. Meta retains this contact data unless deleted by the user and periodically syncs with the user’s devices to capture changes and additions. Users can similarly allow Meta to search an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates.

27. Each Instagram user has a profile page where certain content they create and share (“posts”) can be viewed either by the general public or only the user’s followers, depending on privacy



settings. Users can customize their profile by adding their name, a photo, a short biography (“Bio”), and a website address.

28. One of Instagram’s primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or stored on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of other users (“tag”), or add a location. These appear as posts on the user’s profile. Users can remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Meta’s servers.

29. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can “mention” others by adding their username to a comment followed by “@”). An Instagram post created by one user may appear on the profiles or feeds of other users depending on a number of factors, including privacy settings and which users were tagged or mentioned.

30. An Instagram “story” is similar to a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator’s “Stories Archive” and remain on Meta’s servers unless manually deleted. The usernames of those who viewed a story are visible to the story’s creator until 48 hours after the story was posted.

31. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are removed from Instagram upon completion unless the creator chooses to send the video to IGTV, Instagram’s long-form video app.

32. Instagram Direct, Instagram’s messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos, posts, videos, profiles, and other information. Participants to a group conversation can name the group and send invitations to others to join. Instagram users can send individual or group messages with “disappearing” photos or

videos that can only be viewed by recipients once or twice, depending on settings. Senders can't view their disappearing messages after they are sent but do have access to each message's status, which indicates whether it was delivered, opened, or replayed, and if the recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

33. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform as well as on Facebook and other associated websites and apps. Instagram collects and retains payment information, billing records, and transactional and other information when these services are utilized.

34. Instagram has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily searchable and can be "followed" to generate related updates from Instagram. Meta retains records of a user's search history and followed hashtags.

35. Meta collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Meta to personalize and target advertisements.

36. Meta uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. Meta maintains related records for Instagram users, including information about their perceived ad topic preferences, interactions with ads, and advertising identifiers. This data can provide insights into a user's identity and activities, and it can also reveal potential sources of additional evidence.

37. In some cases, Instagram users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications,

including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

38. For each Instagram user, Meta collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

39. In my training and experience, evidence of who was using Instagram and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

40. The stored communications and files connected to an Instagram account may provide direct evidence of the offenses under investigation. Based on my training and experience, messages, photos, videos, audio messages, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

41. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Meta can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

42. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

43. Other information connected to the use of Instagram may lead to the discovery of additional evidence. For example, the messages stored in Instagram accounts may reveal the identities of co-conspirators. In addition, messages stored in Instagram accounts can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

44. Therefore, Meta's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Instagram. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

#### **PASSWORDS (AND HASHES AND SALT)**

45. The subscriber will also generally need to use a password that will allow the user to gain access to the account. Many providers do not store the password directly, rather they use an algorithm (often referred to as a "hashing" algorithm) that is performed on the password and generates a new random string of numbers and characters, which is what the provider may store. When a user enters his or her password, the hashing algorithm is performed on the password before it is presented to the provider, and the provider will verify the hash value for the password (rather than the password itself) to authorize access to the account. As an added security feature, some providers insert additional text before or after the password, which additional text is referred to as "salting" the password. The hashing algorithm is then performed on the combined password and salt, which is the hash value that will be recognized by the provider. Alternatively or in addition to passwords, users may be required to select or

propose a security question, and then provide an answer, which can be used to substitute for a password or to retrieve or reset a user's password.

### **SEARCH HISTORY**

46. In my training and experience, providers also keep a record of search queries run by the user of the account, whether searches within the services of the provider for persons, content, or other accounts (such as if a user is trying to find the account of an acquaintance), or broader Internet searches. In some instances, providers may also keep records of which websites or contents were "clicked on" as a result of these searches. This information is helpful in the context of the case to show the topics about which the user was trying to obtain more information or conduct research, and is relevant for "user attribution" evidence, analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

### **WEB BROWSING:**

47. I know based on my training and experience that providers of e-mail or social media services generally have access to and store the web or Internet browsing history of the user while he or she is logged into an account. That history can include the names and specific websites or URLs/URIs (Uniform Resource Locators or Indicators) of the sites that have been visited.

### **USER AGENT STRING:**

48. Providers of similar services will often keep track of what is referred to as user agent string, which contains information about the type of computer, operating system, and web browser used to access the service. User agent string can include: web requests or HTTP requests (hypertext transfer protocol is the protocol by which many web pages are transmitted between servers and clients or users); logs containing information such as the requestor's IP address, identity and user ID, date and timestamp, request URL or URI (Uniform Resource Locator or Indicator, i.e., a website address), HTTP protocol version, referrer, and similar information; login tracker logs; account management logs; and any other e-mail or social media accounts accessed by or analytics related to the SUBJECT ACCOUNT. These can



be used to determine the types of devices used while accessing the SUBJECT ACCOUNT, as well as data related to the user's activity while accessing the SUBJECT ACCOUNT.

### **COOKIES**

49. I have also learned that providers of e-mail and social media services often track the behavior and activities of persons using accounts by using cookies, which are strings of characters and numbers stored on a person's computer on their web browser. These cookies can often show whether more than one account was accessed by the same computer (and specifically the same web browser), as the provider can recognize that cookie when the same device returns to the service to access an account.

50. In order to identify other accounts used or maintained by the user of a SUBJECT ACCOUNT, the warrant also calls for the PROVIDER to disclose both (1) any cookies associated with the SUBJECT ACCOUNT, i.e., those cookies that were placed on any computers or web browsers (for example, Internet Explorer or Google Chrome) used to access the SUBJECT ACCOUNT, and (2) the identity of any other account in which the same cookie or cookies used to access the SUBJECT ACCOUNT was/were recognized. If in the course of the investigation the digital devices used by the subject(s) of the investigation are found, they can be searched to determine if the cookies recognized by the provider are stored on those devices. The warrant also calls for the PROVIDER to identify any other accounts accessed by any computer or web browser using the same cookies as the SUBJECT ACCOUNT by providing subscriber records and log-in information for those other accounts (but not to provide the contents of communications in those other accounts).

### **COMMON SUBSCRIBER RECORD INFORMATION**

51. Users of accounts are often required to include an e-mail account as well as a phone number in subscriber records. The e-mail account may be an e-mail account hosted at the same provider, or an account at a different provider. The e-mail account is referred to by a number of names, such as a secondary e-mail account, a recovery e-mail account, or an alternative e-mail account or communication channel. That e-mail account is often used when the identity of the user of the primary account (here, a SUBJECT ACCOUNT) needs to be verified, for example if a password is forgotten, so that the provider

can confirm that the person trying to access the account is the authorized user of the account. Similarly, the telephone number used in subscriber records is often used to send a passcode via text (or “SMS”) that must be presented when trying to gain access to an account, either in a similar scenario where a user forgot his or her password, or when users implement what is referred to as “two-factor authentication” (where the password is one factor, and the passcode sent via text message to a mobile device is a second). In either scenario, the user of a primary e-mail account (a SUBJECT ACCOUNT) and a secondary e-mail account or phone number listed in subscriber records are very often the same person, or at least are close and trusted and/or working in concert. That is because access to either the secondary e-mail account or to the phone number listed in subscriber records can allow access to the primary account.

### **DEVICES**

52. Providers also frequently obtain information about the types of devices that are used to access accounts like the SUBJECT ACCOUNT. Those devices can be laptop or desktop computers, cellular phones, tablet computers, or other devices. Individual computers or devices are identified by a number of different means, some of which are assigned to a particular device by a manufacturer and connected to the “hardware” or the physical device, some are assigned by a cellular telephone carrier to a particular account using cellular data or voice services, and some are actually assigned by the provider to keep track of the devices using its services. Those device identifiers include Android IDs, Advertising IDs, unique application numbers, hardware models, operating system versions, unique device identifiers, Global Unique Identifiers or “GUIDs,” serial numbers, mobile network information, phone numbers, device serial numbers, Media Access Control (“MAC”) addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”). Apple, one of the primary suppliers of mobile devices used to access accounts like the SUBJECT ACCOUNT, had previously used an identifier that was unique to the hardware of its devices, such that details of a device’s activity obtained from a

particular application or “app” could be used to target advertisements for the user of that device. Apple replaced that hardware-based identifier with the Apple advertiser ID or IDFA that is still unique to a particular device, but which can be wiped and re-generated anew by a user if a user chooses to do so. Most users, however, do not know that the IDFA exists, and therefore are unaware that their device’s activity can be correlated across different apps or services. Google uses a similar advertiser ID referred to as an AAID.

53. These device identifiers can then be used (a) to identify accounts accessed at other providers by that same device, and (b) to determine whether any physical devices found in the course of the investigation were the ones used to access a SUBJECT ACCOUNT. The requested warrant therefore asks for the device identifiers, as well as the identity of any other account accessed by a device with the same identifier.

#### **LOCATION INFORMATION**

54. Providers of e-mail and social media often maintain, have access to, and store information related to the location of the users of accounts they service. That information may be obtained by the provider in a number of ways. For example, a user may access the provider’s services by running an application on the user’s phone or mobile device, which application has access to the location information residing on the phone or mobile device, such as Global Positioning System (GPS) information. It may also be accessible through “check-in” features that some providers offer that allow users to transmit or display their location to their “friends” or “acquaintances” via the provider.

#### **REQUEST FOR SEALING**

55. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet and disseminate them to other

online criminals as they deem appropriate, i.e., post them publicly online. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

### **REQUEST FOR NON-DISCLOSURE**

56. Request for Order Barring Notification of Other Persons (Non-Disclosure Order): In addition, pursuant to 18 U.S.C. § 2705(b), I would request the Court order the Target Providers described in Attachment A not to notify any other person, including the subscribers or customers of the account(s) listed in Attachment A, of the existence of this warrant, its contents, and any information provided in response thereto, until one year from the date of this warrant, and to continue to maintain the accounts in an open and active status so as not to disrupt this ongoing investigation.

57. As described above, this warrant relates to an ongoing investigation into drug and firearms offenses. Subjects of such investigations frequently engage in extensive online social networking, including efforts to discover any potential ongoing investigations relating to them. This investigation is neither public nor known to all of the subjects of the investigation, and its disclosure may alert the subjects to the ongoing investigation. Notification of this investigation provides an opportunity for the subjects to flee prosecution. Additionally, some of the evidence in this investigation is stored electronically. If alerted to the investigation, the subjects under investigation could destroy any evidence saved on their electronic devices, including information saved to their personal computers, as subjects have done in similar types of investigations when alerted to the investigation. Moreover, notification of the subscriber or customer will likely result in the subjects changing patterns of behavior and/or discontinuing use of a particular means for committing the crime, therefore seriously jeopardizing the investigation.

58. Accordingly, there is reason to believe that notification of the existence of the warrant, its contents, and the information requested therein, will seriously jeopardize the investigation, including by giving subjects an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates. See 18 U.S.C. §§ 2705(b)(2), (3), and (5)

### INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

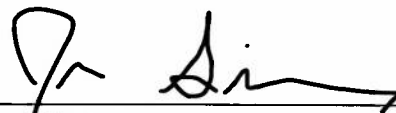
59. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Meta to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

### CONCLUSION

60. Based on the foregoing, I request that the Court issue the proposed search warrant.

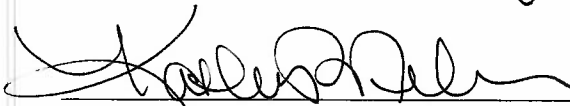
61. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Meta Platforms, Inc. Because the warrant will be served on Meta Platforms, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Joseph Simmons  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me on January 25, 2024



UNITED STATES MAGISTRATE JUDGE 4:00pm



**ATTACHMENT A**

***PROPERTY TO BE SEARCHED***

This warrant applies to information associated with the Instagram accounts with username: **Yfg.Huncho** and **Huncho2litt** that are stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. a company headquartered in Menlo Park, CA.

## **ATTACHMENT B**

### **PARTICULAR THINGS TO BE SEIZED**

#### **I. Information to be disclosed by Meta Platforms, Inc. ("Meta")**

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, including any emails, messages, records, files, logs, or information that have been deleted but are still available to Meta, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each account listed in Attachment A:

##### **A. All business records and subscriber information, in any form kept, pertaining to the Account, including:**

1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;
2. All Instagram usernames (past and current) and the date and time each username was active, all associated Instagram and Facebook accounts (including those linked by machine cookie), and all records or other information about connections with Facebook, third-party websites, and mobile apps (whether active, expired, or removed);
3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;
4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;
5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;

6. Internet Protocol ("IP") addresses used to create, login, and use the account, including associated dates, times, and port numbers, from January 1, 2022 to current date;
  7. Privacy and account settings, including change history; and
  8. Communications between Meta and any person regarding the account, including contacts with support services and records of actions taken;
- B. All content (whether created, uploaded, or shared by or with the Account), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata, from January 1, 2022 to current date; ;
- C. All content, records, and other information relating to communications sent from or received by the Account from January 1, 2022 to current date; , including but not limited to:
1. The content of all communications sent from or received by the Account, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;
  2. All records and other information about direct, group, and disappearing messages sent from or received by the Account, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);
  3. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and
  4. All associated logs and metadata;
- D. All content, records, and other information relating to all other interactions between the Account and other Instagram users from January 1, 2022 to current date; , including but not limited to:

1. Interactions by other Instagram users with the Account or its content, including posts, comments, likes, tags, follows (including unfollows, approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;
  2. All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;
  3. All contacts and related sync information; and
  4. All associated logs and metadata;
- E. All records of searches performed by the account from January 1, 2022 to current date; and
- F. All location information, including location history, login activity, information geotags, and related metadata from January 1, 2022 to current date;

Meta is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

**II. Information to be seized by the government**

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 18 U.S.C § 922 and 924: Shipping, Transporting, Receiving, or Possessing Firearms or Ammunition, 18 U.S.C § 924(c)(1): Use of a firearm in furtherance of a drug trafficking, 21 U.S.C. § 841(a)(1): Manufacturing, Distributing, Dispensing or Possessing With Intent to Manufacture, Distribute or Dispense Controlled Substances, and 21 U.S.C. § 846: Conspiracy to Commit a Title 21 Offense (“Target Offenses”), those violations involving an unknown suspect or suspects associated with the information to be searched and occurring after January 1, 2022 , including, for each Account or identifier listed on Attachment A, information pertaining to the following matters:

- a. All evidence related to the acquisition, possession, or sale of narcotics and/or machinegun conversion devices;

- b. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- c. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;
- d. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).
- e. The identity of the person(s) who communicated with the Account about matters relating to the Target Offenses including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.